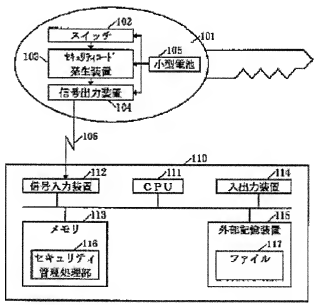
COMPUTER ILLEGAL USE PREVENTION DEVICE

Publication number: JP9171416
Publication date: 1997-06-30
Inventor: SUZUKI HITOSHI; UEHARA MINORU; FURUYUI AKIO
Applicant: HITACHI LTD
Classification:
- international: ***G06F1/00; G06F12/14; G06F15/00; G06F21/20;*** **G06F1/00; G06F12/14; G06F15/00; G06F21/20;** (IPC1-7): G06F1/00; G06F15/00
- European:
Application number: JP19960212276 19960812
Priority number(s): JP19960212276 19960812; JP19950271161 19951019

Report a data error here

Abstract of **JP9171416**

PROBLEM TO BE SOLVED: To improve the operability of a security management preventing computer illegal use by providing a security key with a signal output device outputting a security code and providing a security management processing part executing and permitting a function when a security code signal is inputted and this signal is a valid security code on a computer main body. SOLUTION: This device is provided with a security key 101, a switch 102, a security code generator 103, a signal output device 104, a small-sized battery 105, a security code signal 106, a computer 110, a CPU 111, a signal input device 112, a memory 113, an input/output device 114, an external storage 115, a security control processing part 116 and a file 117. Unique codes are preliminarily stored in a read only memory, etc., provided on a security code generator 103 and these codes are generated as security codes.



Data supplied from the ***esp@cenet*** database - Worldwide

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号

特開平9－171416

(43)公開日　平成９年(1997)６月30日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｇ０６Ｆ　1/00	３７０		Ｇ０６Ｆ　1/00	３７０Ｅ	
15/00	３３０		15/00	３３０Ｇ	

審査請求　未請求　請求項の数３　ＯＬ　（全 20 頁）

(21)出願番号　特願平8－212276

(22)出願日　平成８年(1996)８月12日

(31)優先権主張番号　特願平7－271161

(32)優先日　平７(1995)10月19日

(33)優先権主張国　日本（ＪＰ）

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地

(72)発明者　鈴木　仁
神奈川県海老名市下今泉810番地　株式会社日立製作所オフィスシステム事業部内

(72)発明者　上原　実
神奈川県海老名市下今泉810番地　株式会社日立製作所オフィスシステム事業部内

(72)発明者　古結　明男
神奈川県海老名市下今泉810番地　株式会社日立製作所オフィスシステム事業部内

(74)代理人　弁理士　秋田　収喜

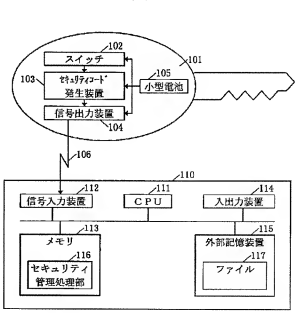
(54)【発明の名称】　コンピュータ不正使用防止装置

(57)【要約】

【課題】　コンピュータの不正使用を防止するセキュリティ管理の操作性を向上することが可能な技術を提供する。

【解決手段】　ユニークなセキュリティコードを発生するセキュリティコード発生装置と、前記セキュリティコードをセキュリティコード信号に変換して前記セキュリティコードを出力する信号出力装置とをセキュリティキーに備え、前記セキュリティコード信号を入力して前記セキュリティコードに変換する信号入力装置と、前記変換されたセキュリティコードと登録リストに登録された複数の有効なセキュリティコードとを比較し、前記変換されたセキュリティコードが有効なセキュリティコードである場合に前記セキュリティコードに対応する機能の実行を許可するセキュリティ管理処理部とをコンピュータ本体に備えるものである。

図１



【特許請求の範囲】
【請求項１】　非接触型または接触型のセキュリティキーを利用したコンピュータの不正使用を防止するコンピュータ不正使用防止装置であって、
ユニークなセキュリティコードを発生するセキュリティコード発生装置と、前記セキュリティコードをセキュリティコード信号に変換して前記セキュリティコードを出力する信号出力装置とをセキュリティキーに備え、
前記セキュリティコード信号を入力して前記セキュリティコードに変換する信号入力装置と、前記変換されたセキュリティコードと登録リストに登録された複数の有効なセキュリティコードとを比較し、前記変換されたセキュリティコードが有効なセキュリティコードである場合に前記セキュリティコードに対応する機能の実行を許可するセキュリティ管理処理部とをコンピュータ本体に備えることを特徴とするコンピュータ不正使用防止装置。
【請求項２】　コンピュータ本体からの信号を入力する信号入力装置をセキュリティキーに備え、セキュリティキーに信号を出力する信号出力装置をコンピュータ本体に備えることを特徴とする請求項１に記載されたコンピュータ不正使用防止装置。
【請求項３】　ネットワークを介してセキュリティコードを送信するセキュリティコード送信部と、ネットワークを介して送信されたセキュリティコードを受信するセキュリティコード受信部とをネットワークに接続された複数のコンピュータ本体に備え、
特定のコンピュータのセキュリティコード送信部からネットワークに接続された他のコンピュータのセキュリティコード受信部にセキュリティコードを送信し、前記送信したセキュリティコードを使用して前記他のコンピュータのセキュリティ管理処理を実行することを特徴とする請求項１または請求項２のいずれかに記載されたコンピュータ不正使用防止装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、非接触型または接触型のセキュリティキーによりコンピュータの不正使用を防止するコンピュータ不正使用防止装置に関し、特に、セキュリティキーから送られたセキュリティコードに応じてコンピュータの特定の機能の実行を許可するコンピュータ不正使用防止装置に適用して有効な技術に関するものである。
【０００２】
【従来の技術】近年、コンピュータを使用した業務が増加するにつれて、会社の機密に関するデータや個人のプライバシーに関するデータ等、機密保護を必要とする多量のデータがコンピュータに蓄積されてきている。
【０００３】従来のコンピュータに蓄積されたデータの機密保護に関しては、「電子情報通信ハンドブック、電子情報通信学会編」等に記載されており、コンピュータに蓄積されたデータの暗号化、コンピュータの利用者の利用資格の確認を行うユーザ認証、データが改ざんされていないことを確認するデータ認証及び記憶装置上の他のプログラムやデータを保護する記憶保護がある。
【０００４】前記従来のコンピュータに蓄積されたデータの機密保護の内、コンピュータの利用者の利用資格を確認し、コンピュータの不正使用を防止するユーザ認証には、（ａ）パスワードを使用する方法、（ｂ）フロッピーディスクやＰＣカードなどの取り外し可能な記憶媒体を用いる方法、（ｃ）磁気カード等の専用入出力装置を必要とする記憶媒体を用いる方法、及び、（ｄ）物理的な鍵を使用する方法がある。
【０００５】前記（ａ）のパスワードを使用する方法は、利用者を識別するユーザＩＤと利用者本人しか知ることのできないパスワードをコンピュータ内に格納し、利用者がコンピュータを使用する際に、その利用者のユーザＩＤとパスワードを入力し、入力されたパスワードと前記コンピュータ内に格納されているパスワードとを比較し、入力されたパスワードが前記コンピュータ内に格納されているパスワードと一致するときに、そのパスワードを入力した利用者が正規の利用者本人であるとみなす方法である。
【０００６】前記（ｂ）のフロッピーディスクやＰＣカードなどの取り外し可能な記憶媒体を用いる方法は、利用者がコンピュータに装着したフロッピーディスクやＰＣカード等の取り外し可能な記憶媒体に格納されたデータを読み出し、そのデータが予めコンピュータ内部に格納されているデータと一致するときに、その記憶媒体を装着した利用者が正規の利用者本人であるとみなす方法である。
【０００７】前記（ｃ）の磁気カード等の専用入出力装置を必要とする記憶媒体を用いる方法は、利用者の磁気カード等の記憶媒体に格納されたデータを専用入出力装置によって読み出し、その読み出したデータが予めコンピュータ内部に格納されているデータと一致するときに、その記憶媒体を所持している利用者が正規の利用者本人であるとみなす方法である。
【０００８】前記（ｄ）の物理的な鍵を使用する方法は、コンピュータを設置した部屋やコンピュータの電源スイッチ等を物理的な鍵を使用して施錠し、前記コンピュータを使用する際には、物理的な鍵を使用してコンピュータを設置した部屋やコンピュータの電源スイッチ等の施錠を解除する方法である。
【０００９】
【発明が解決しようとする課題】本発明者は、前記従来技術を検討した結果、以下の問題点を見い出した。
【００１０】すなわち、前記（ａ）のパスワードを使用する方法では、コンピュータの利用者がパスワードをメモ用紙に記録したり、他の人に記憶してもらったり、記憶しやすいコードにすることがある為、パスワードが利

用者本人以外に漏洩しやすいという問題があった。

【００１１】また、前記（ａ）のパスワードを使用する方法では、異なるユーザＩＤで同じパスワードを使用することができる為、パスワードは必ずしもユニークとはならず、偶然に漏洩する可能性があるという問題があった。

【００１２】前記（ａ）のパスワードを使用する方法で、定期的にパスワードを切り替えることによりパスワードの漏洩を防止した場合には、漏洩はしにくくなるもののパスワードを忘れる可能性は更に高くなるという問題があった。

【００１３】前記（ｂ）のフロッピーディスクやＰＣカード等の取り外し可能記憶媒体を用いる方法では、コンピュータのフロッピーディスクやＰＣカードの装着スロットがコンピュータの不正使用を防止するセキュリティキーとしての用途に占有され、他の用途に使用できなくなるという問題と、フロッピーディスクやＰＣカードを装着スロットに頻繁に装着することにより摩耗が発生し、フロッピーディスクやＰＣカードのデータを読み取る信頼性が低下したり、フロッピーディスクやＰＣカードを装着スロットに装着したまま忘れて他の人に盗難されたり、そのままコンピュータを不正に使用されてしまう危険性が高いという問題があった。

【００１４】また、フロッピーディスクは携帯は可能であるが、自動車の鍵や家の鍵の様に常に身に付けておくには不便であると共に複製が容易である為、漏洩しやすいという問題があり、ＰＣカードは他の記憶媒体と比較して高価な為、現用のキーの他に予備のキーを設けたり、１台のコンピュータを複数の利用者で共用する為に複数のセキュリティキーを設けたり、コンピュータの管理の為に管理者用のキーと利用者用のキーの様に複数のセキュリティキーを設けたりする場合に、他の記憶媒体よりも多くの費用がかかるという問題があった。

【００１５】前記（ｃ）の磁気カード等の専用入出力装置が必要な記憶媒体を用いる方法では、コンピュータに専用入出力装置を接続する必要がある為、多くの費用がかかるという問題と、ノート型コンピュータなど携帯性を生かしたコンピュータでは専用入出力装置の接続により携帯性が著しく損なわれてしまうという問題があった。

【００１６】前記（ｄ）の物理的な鍵を使用する方法では、鍵を装着したまま忘れて他の人に盗難されたり、そのままコンピュータを不正に使用されてしまう危険性が高いという問題と、鍵の複製が簡単な反面、現用のキーを無効化し予備のキーに切り替えることや、１台のコンピュータを複数の利用者で共用する為に複数のセキュリティキーを設けたり、コンピュータの管理の為に管理者用のキーと利用者用のキーの様に複数のセキュリティキーを設けたりするのが困難であるという問題があった。

【００１７】本発明の目的は、コンピュータの不正使用を防止するセキュリティ管理の操作性を向上することが可能な技術を提供することにある。

【００１８】本発明の他の目的は、セキュリティの強度を向上せさることが可能な技術を提供することにある。

【００１９】本発明の他の目的は、セキュリティキーからのセキュリティコード信号を入力するインタフェースを備えていないコンピュータに対してもセキュリティ管理を行うことが可能な技術を提供することにある。

【００２０】本発明の前記並びにその他の目的と新規な特徴は、本明細書の記述及び添付図面によって明かになるであろう。

【００２１】

【課題を解決するための手段】本願によって開示される発明のうち、代表的なものの概要を簡単に説明すれば、下記のとおりである。

【００２２】（１）非接触型または接触型のセキュリティキーを利用したコンピュータの不正使用を防止するコンピュータ不正使用防止装置であって、ユニークなセキュリティコードを発生するセキュリティコード発生装置と、前記セキュリティコードをセキュリティコード信号に変換して前記セキュリティコードを出力する信号出力装置とをセキュリティキーに備え、前記セキュリティコード信号を入力して前記セキュリティコードに変換する信号入力装置と、前記変換されたセキュリティコードと登録リストに登録された複数の有効なセキュリティコードとを比較し、前記変換されたセキュリティコードが有効なセキュリティコードである場合に前記セキュリティコードに対応する機能の実行を許可するセキュリティ管理処理部とをコンピュータ本体に備えるものである。

【００２３】前記コンピュータ不正使用防止装置では、まず、前記セキュリティキーのスイッチを押すことにより、前記セキュリティコード発生装置からユニークなセキュリティコードを発生する。

【００２４】次に、前記セキュリティキーの信号出力装置は、前記発生したセキュリティコードを特定のセキュリティコード信号、例えば、赤外線信号に変換し、前記変換したセキュリティコード信号をコンピュータの信号入力装置に出力する。

【００２５】このとき、前記セキュリティキーのセキュリティコード発生装置及び信号出力装置への給電は、前記セキュリティキーに備えられた小型電池によって行われる。

【００２６】前記コンピュータの信号入力装置は常時予備電源により動作し、前記セキュリティキー側の信号出力装置から送られてきたセキュリティコード信号を、コンピュータ側の信号入力装置で入力してセキュリティコードに変換する。

【００２７】次に、前記コンピュータのセキュリティ管理処理部は、予め有効なセキュリティコードを登録した登録リストを参照し、前記変換したセキュリティコード

と前記登録リスト中のセキュリティコードとを比較して、前記変換したセキュリティコードが有効なセキュリティコードであるかどうかの照合判定を行う。

【００２８】前記変換したセキュリティコードが有効なセキュリティコードである場合には、前記セキュリティコードに対応する特定の機能の実行を許可し、また、前記変換したセキュリティコードが有効なセキュリティコードでない場合には、前記コンピュータの使用を禁止する。

【００２９】前記変換したセキュリティコードが有効なセキュリティコードである場合に許可する機能としては、コンピュータ本体の主電源の投入、以前いロックされた入力操作の再開、前記コンピュータ内の情報に対する参照、移動、複写、変更、暗号化及び復号化の操作等が挙げられる。

【００３０】前記コンピュータ不正使用防止装置のセキュリティキーは、ユニークなセキュリティコードを発生するセキュリティコード発生装置と、例えば、今後のコンピュータでは標準的に装備される赤外線インタフェースを備えた信号出力装置と、前記セキュリティコード発生装置及び信号出力装置に電源を供給する小型電池と、スイッチとから構成することにより、小型で低コストかつ非接触型とすることが可能である。

【００３１】前記の様に、コンピュータに標準的に装備される赤外線インタフェースを使用することにより、コンピュータのフロッピーディスク等の装着スロットの専用機器による占有や前記専用機器搭載によるコストアップを伴うことなく、コンピュータの不正使用を防止することが可能である。

【００３２】また、セキュリティキーを小型で低コストにし、コンピュータ本体への専用機器搭載によるコストアップをなくしたことから、予備のセキュリティキー、１台のコンピュータを複数の利用者で共用する際の複数のセキュリティキー、または、コンピュータの管理を行う際に使用する管理者用セキュリティキーと管理以外の処理の際に使用する利用者用セキュリティキーの様に用途別の複数のセキュリティキーを設けることが容易である。

【００３３】以上の様に、前記コンピュータ不正使用防止装置によれば、発生したユニークなセキュリティコードを出力してコンピュータのセキュリティ管理を行うので、コンピュータの不正使用を防止するセキュリティ管理の操作性を向上することが可能である。

【００３４】（２）前記（１）に記載されたコンピュータ不正使用防止装置において、コンピュータ本体からの信号を入力する信号入力装置をセキュリティキーに備え、セキュリティキーに信号を出力する信号出力装置をコンピュータ本体に備えるものである。

【００３５】前記コンピュータ不正使用防止装置では、例えば、ＩＣカードで構成されたセキュリティキーのセキュリティコード発生装置から発生されたユニークなセキュリティコードを特定のセキュリティコード信号に変換し、前記変換したセキュリティコード信号をコンピュータの信号入力装置に出力する。

【００３６】前記コンピュータの信号入力装置は、前記セキュリティキー側の信号出力装置から送られてきたセキュリティコード信号を入力してセキュリティコードに変換し、前記コンピュータのセキュリティ管理処理部は、登録リストを参照して、前記変換したセキュリティコードが有効なセキュリティコードであるかどうかの照合判定を行う。

【００３７】前記変換したセキュリティコードが有効なセキュリティコードである場合には、前記セキュリティコードに対応する特定の機能の実行を許可し、また、前記変換したセキュリティコードが有効なセキュリティコードでない場合には、前記コンピュータの使用を禁止する。

【００３８】前記セキュリティ管理処理部は、前記変換したセキュリティコードが有効なセキュリティコードである場合に、セキュリティコードを変更する機能が選択されると、前記登録リスト中のセキュリティコードを変更するとと共に、前記コンピュータの信号出力装置により、前記変更したセキュリティコードをセキュリティコード信号に変換してセキュリティキーに出力する。

【００３９】前記セキュリティキーの信号入力装置は、前記コンピュータ本体側の信号出力装置から送られてきたセキュリティコード信号を入力してセキュリティコードに変換し、前記変換したセキュリティコードを使用してセキュリティキーのセキュリティコード発生装置が発生するセキュリティコードを変更する。

【００４０】また、前記の様にＩＣカードを使用してセキュリティキーを高機能化し、コンピュータ本体の信号出力装置及びセキュリティキーの信号入力装置を使用することにより、コンピュータ本体の使用履歴情報や障害情報をセキュリティキーに蓄積したり、また、セキュリティ管理だけでなく、勤怠情報を蓄積して勤怠管理に使用したり、製品情報を蓄積して在庫管理に使用し、また、現金情報を蓄積して電子マネーと兼用することが可能である。

【００４１】以上の様に、前記コンピュータ不正使用防止装置によれば、コンピュータの信号出力装置により変更したセキュリティコードをセキュリティキーに出力し、セキュリティキーのセキュリティコードを変更するので、セキュリティの強度を向上せさることが可能である。

【００４２】（３）前記（１）または（２）に記載されたコンピュータ不正使用防止装置において、ネットワークを介してセキュリティコードを送信するセキュリティコード送信部と、ネットワークを介して送信されたセキュリティコードを受信するセキュリティコード受信部と

をネットワークに接続された複数のコンピュータ本体に備え、特定のコンピュータのセキュリティコード送信部からネットワークに接続された他のコンピュータのセキュリティコード受信部にセキュリティコードを送信し、前記送信したセキュリティコードを使用して前記他のコンピュータのセキュリティ管理処理を実行するものである。

【００４３】前記コンピュータ不正使用防止装置では、セキュリティキーから受信したセキュリティコードが有効なセキュリティコードである場合に、他のコンピュータのセキュリティ管理を実行する機能が選択されると、前記セキュリティコード送信部により、前記セキュリティキーから受信済みの有効なセキュリティコードをネットワークに接続された他のコンピュータに送信する。

【００４４】前記ネットワークに接続された他のコンピュータは、セキュリティコード受信部によりセキュリティコードを受信した後、当該コンピュータのセキュリティ管理処理部を起動する。

【００４５】前記セキュリティコード送信部によりセキュリティコードを送信したコンピュータは、前記起動された他のコンピュータのセキュリティ管理処理部に、セキュリティ管理に関する指示を送り、当該コンピュータのセキュリティ管理機能を実行する。

【００４６】以上の様に、前記コンピュータ不正使用防止装置によれば、ネットワークに接続された他のコンピュータのセキュリティ管理処理を実行するので、セキュリティキーからのセキュリティコード信号を入力するインタフェースを備えていないコンピュータに対してもセキュリティ管理を行うことが可能である。

【００４７】

【発明の実施の形態】

（実施形態１）以下に、本発明のコンピュータ不正使用防止装置において、赤外線の非接触型セキュリティキーを使用する実施形態１のコンピュータ不正使用防止装置について説明する。

【００４８】図１は、本実施形態のコンピュータ不正使用防止装置の概略構成を示す図である。図１において、１０１はセキュリティキー、１０２はスイッチ、１０３はセキュリティコード発生装置、１０４は信号出力装置、１０５は小型電池、１０６はセキュリティコード信号、１１０はコンピュータ、１１１はＣＰＵ、１１２は信号入力装置、１１３はメモリ、１１４は入出力装置、１１５は外部記憶装置、１１６はセキュリティ管理処理部、１１７はファイルである。

【００４９】図１に示す様に、本実施形態のコンピュータ不正使用防止装置は、セキュリティキー１０１と、スイッチ１０２と、セキュリティコード発生装置１０３と、信号出力装置１０４と、小型電池１０５と、セキュリティコード信号１０６と、コンピュータ１１０と、ＣＰＵ１１１と、信号入力装置１１２と、メモリ１１３と、入出力装置１１４と、外部記憶装置１１５と、セキュリティ管理処理部１１６と、ファイル１１７とを有している。

【００５０】また、図１に示す様に、本実施形態のコンピュータ不正使用防止装置では、セキュリティキー１０１として、小型、低コストで、キーホルダー等に付け、常にコンピュータ１１０の管理者の身に付けて不便のないものが作成可能であり、複数のセキュリティキー１０１を作成することにより、１個を現用セキュリティキー、他を予備セキュリティキーとして用意することが低コストで可能になる。

【００５１】本実施形態のコンピュータ不正使用防止装置では、セキュリティコード発生装置１０３に備えられたリードオンリメモリ等に予めユニークなコードを記憶しておき、これをセキュリティコードとして発生させており、ユニークなコードと変化するコード、例えば日付時刻などを合成したコードをセキュリティコードとして使用することにより、セキュリティコード信号１０６の不正な複製を困難にすることが可能である。

【００５２】本実施形態のコンピュータ不正使用防止装置の信号出力装置１０４及び信号入力装置１１２は、今後のパーソナルコンピュータで標準的に装備される赤外線インタフェース（ＩｒＤＡ：Ｉｎｆｒａ　ｒｅｄ　Ｄａｔａ　Ａｓｓｏｃｉａｔｉｏｎ）を使用し、また、セキュリティ管理処理部１１６は、パスワードによるセキュリティの管理機能と同様にソフトウェアで実現する。

【００５３】本実施形態のコンピュータ不正使用防止装置では、ユニークなセキュリティコードを発生するセキュリティコード発生装置１０３、赤外線インタフェースを持つ信号入力装置１１２、小型電池１０５及びスイッチ１０２により、セキュリティキー１０１を小型、低コストかつ非接触型とし、コンピュータ１１０のフロッピーディスク等の装着スロットの専用機器による占有や前記専用機器搭載によるコストアップをなくしている。

【００５４】この為、本実施形態のコンピュータ不正使用防止装置では、予備セキュリティキーや、１台のコンピュータ１１０を複数の利用者で共用する際の様にセキュリティキー１０１を複数としたり、また、コンピュータ１１０の管理の際に使用する管理者用セキュリティキーと管理以外の処理に使用する利用者用セキュリティキーの様にセキュリティキー１０１を複数設けることが容易である。

【００５５】更に、本実施形態のコンピュータ不正使用防止装置では、１人の利用者が複数台のコンピュータ１１０を操作あるいは管理する場合には、複数台のコンピュータ１１０に対して１つのセキュリティキー１０１を共通に登録することも可能である。

【００５６】図２は、本実施形態のコンピュータ不正使用防止装置のセキュリティ管理処理部１１６の概略構成を示す図である。図２において、２０１は登録処理機

能、２０２は変更処理機能、２０３はシステム起動ロック処理機能、２０４は中断再開ロック処理機能、２０５はアプリケーション起動ロック処理機能、２０６はファイルロック処理機能、２０７は暗号化処理機能、２０８は復号化処理機能、２０９は使用状況の履歴取得処理機能、２１０は登録リストである。

【００５７】図２に示す様に、本実施形態のコンピュータ不正使用防止装置のセキュリティ管理処理部１１６は、登録処理機能２０１と、変更処理機能２０２と、システム起動ロック処理機能２０３と、中断再開ロック処理機能２０４と、アプリケーション起動ロック処理機能２０５と、ファイルロック処理機能２０６と、暗号化処理機能２０７と、復号化処理機能２０８と、使用状況の履歴取得処理機能２０９と、登録リスト２１０とを有している。

【００５８】また、図２に示す様に、本実施形態のコンピュータ不正使用防止装置のセキュリティ管理処理部１１６では、登録リスト２１０に登録された内容により、対応する処理機能の実行を管理している。

【００５９】登録処理機能２０１は、登録リスト２１０にセキュリティコードが登録されていない場合、登録リスト２１０にセキュリティキー１０１からのセキュリティコードを登録する機能であり、複数のセキュリティコードの登録や、セキュリティキー１０１ごとに有効範囲、すなわち、当該セキュリティコードによって実行できるセキュリティ管理処理部１１６の機能の範囲、およびコンピュータ操作環境（画面環境、ファイル環境、アプリケーション環境等）の登録を行う機能である。

【００６０】変更処理機能２０２は、登録リスト２１０にセキュリティコードが既に登録されている場合に登録リスト２１０に登録されている有効なセキュリティコードを受信すると、登録リスト２１０の変更を許可する機能であり、例えばセキュリティコードの追加登録、登録抹消、有効範囲の変更、コンピュータ操作環境等の変更を行う機能である。

【００６１】システム起動ロック処理機能２０３は、登録リスト２１０にセキュリティコードが登録されているときに、登録リスト２１０に登録されている有効なセキュリティコードが受信されない場合にはコンピュータ１１０の電源の投入及びシステム起動を禁止し、有効なセキュリティコードが受信された場合には、そのセキュリティコードに対応して予め設定したコンピュータ操作環境への切り替えを行う機能である。

【００６２】中断再開ロック処理機能２０４は、登録リスト２１０にセキュリティコードが登録されているときに、一定時間中に入出力装置１１４のキーボードやマウス等からの入力が無く、コンピュータ１１０への操作が行われなかった場合に、コンピュータ１１０への操作が中断されているとみなして入出力装置１１４のディスプレイの画面を消去し、入出力装置１１４のキーボードやマウス等からの入力動作をロックし、登録リスト２１０に登録されている有効なセキュリティコードを受信するまでコンピュータ１１０の入出力装置１１４からの入力動作を中断する機能である。

【００６３】アプリケーション起動ロック処理機能２０５は、登録リスト２１０にセキュリティコードが登録されている場合に、コンピュータ１１０内あるいはネットワークで接続された他のコンピュータ内の予め設定されたアプリケーションソフトウェアを起動しようとしたときに、登録リスト２１０に登録されている有効なセキュリティコードを受信するまでの間、当該アプリケーションソフトウェアの起動を停止する機能である。

【００６４】ファイルロック処理機能２０６は、登録リスト２１０にセキュリティコードが登録されている場合に、コンピュータ１１０内あるいはネットワークで接続された他のコンピュータ内の予め設定されたファイル１１７に対して参照、移動、複写、変更などの操作を行おうとしたときに、登録リスト２１０に登録されている有効なセキュリティコードを受信するまでの間、ファイル１１７への操作を停止する機能である。

【００６５】暗号化処理機能２０７は、コンピュータ１１０内あるいはネットワークで接続された他のコンピュータ内のファイル１１７や通信電文などを暗号化するときに、セキュリティキー１０１からのセキュリティコードに基づいて暗号化を行う機能である。

【００６６】復号化処理機能２０８は、コンピュータ１１０内あるいはネットワークで接続された他のコンピュータ内の暗号化されたファイル１１７や通信電文などを復号化するときに、セキュリティキー１０１からのセキュリティコードに基づいて復号化を行う機能である。

【００６７】使用状況の履歴取得処理機能２０９は、登録リスト２１０にセキュリティコードが登録されている場合に、登録リスト２１０に登録されている有効なセキュリティコードを受信していない間のコンピュータ１１０の使用状況の履歴を記憶する機能である。

【００６８】図３は、本実施形態のコンピュータ不正使用防止装置のセキュリティコードの登録処理の処理手順を示すフローチャートである。

【００６９】図３に示す様に、本実施形態のコンピュータ不正使用防止装置のセキュリティコードの登録処理では、ステップ３０１の処理で、コンピュータ１１０のセキュリティ管理処理部１１６の登録処理機能２０１を呼び出し、セキュリティコードの登録処理機能２０１を起動する。

【００７０】ステップ３０２の処理で、セキュリティキー１０１の信号出力装置１０４から送信されたセキュリティコード信号１０６をコンピュータ１１０の信号入力装置１１２で受信し、ステップ３０３の処理で、受信したセキュリティコード信号１０６をセキュリティコードに変換して登録リスト２１０に登録する。

【００７１】ステップ３０４の処理では、ステップ３０３の処理で登録したセキュリティコードに、当該セキュリティコードで実行できるセキュリティ管理処理部１１６を示す有効範囲を設定する。この有効範囲の設定により、コンピュータ１１０を管理する管理者と一般の利用者とをそのセキュリティコードによって区別し、実行できるセキュリティ管理処理部１１６を受信されたセキュリティコードに応じて変更する。

【００７２】ステップ３０５の処理では、ステップ３０３の処理で登録したセキュリティコードに、当該セキュリティコードを受信したときのコンピュータ操作環境を設定する。このコンピュータ操作環境の設定により、コンピュータ１１０でセキュリティコードを受信してコンピュータ１１０の使用を開始したときに、コンピュータ１１０の操作環境を受信したセキュリティコードに応じて特定の操作環境に変更する。

【００７３】複数のセキュリティコードを登録する場合には、ステップ３０６の処理で、次のセキュリティキー１０１の信号出力装置１０４からコンピュータ１１０の信号入力装置１１２へ、次のセキュリティコード信号１０６を送信し、登録リスト２１０に登録し、以下これを繰り返す。

【００７４】本実施形態のコンピュータ不正使用防止装置において、前記の様にセキュリティコードの登録処理を行うと、登録リスト２１０には、「セキュリティコード１」、「セキュリティコード２」等の複数のセキュリティコードと、各セキュリティコードに対応する「処理機能１」、「処理機能２」等の複数の処理機能が登録される。

【００７５】ここで、登録リスト２１０に登録される「処理機能１」、「処理機能２」等の複数の処理機能の内容は、対応するセキュリティコードが入力されたときに実行可能な複数の処理機能を有効範囲として示すと共に、当該処理機能を実行する際の操作環境を表しているものとする。

【００７６】本実施形態のコンピュータ不正使用防止装置では、手元にあるセキュリティキー１０１からのセキュリティコード信号１０６を直接コンピュータ１１０に送信して登録するので、誤って違うコードを登録してしまうミスを防止することが可能である。

【００７７】図４は、本実施形態のコンピュータ不正使用防止装置のセキュリティコードの変更処理の処理手順を示すフローチャートである。

【００７８】図４に示す様に、本実施形態のコンピュータ不正使用防止装置のセキュリティコードの変更処理では、ステップ４０１の処理で、コンピュータ１１０のセキュリティ管理処理部１１６の変更処理機能２０２を呼び出し、セキュリティコードの変更処理機能２０２を起動する。

【００７９】ステップ４０２の処理で、セキュリティキー１０１の信号出力装置１０４から送信したセキュリティコード信号１０６をコンピュータ１１０の信号入力装置１１２で受信し、ステップ４０３の処理で、受信したセキュリティコードと登録リスト２１０に登録されているセキュリティコードとを比較する。

【００８０】ステップ４０３の処理で、受信したセキュリティコードと登録リスト２１０に登録されているセキュリティコードとを比較した結果、受信したセキュリティコードが登録リスト２１０に登録されている有効なセキュリティコードである場合には、コンピュータ１１０のセキュリティ管理処理部１１６は、登録リスト２１０の変更を許可する。

【００８１】ステップ４０４の処理で、セキュリティコードを追加登録する処理を選択した場合には、ステップ４１４の処理に進み、追加したいセキュリティキー１０１の信号出力装置１０４からコンピュータ１１０の信号入力装置１１２へセキュリティコード信号１０６を送信し、送信されたセキュリティコードを登録リスト２１０に登録する。登録リスト２１０に追加登録されたセキュリティコードには、セキュリティコードごとに有効範囲やコンピュータ操作環境を設定することが可能である。

【００８２】ステップ４０５の処理で、セキュリティコードの登録抹消を行う処理を選択した場合には、ステップ４１５の処理に進み、登録抹消したいセキュリティコードを指定して登録リスト２１０から消去する。

【００８３】ステップ４０６の処理で、セキュリティコードの有効範囲を変更する処理を選択した場合には、ステップ４１６の処理に進み、有効範囲を変更したいセキュリティコードを指定し、変更した有効範囲を登録リスト２１０に登録しなおす。

【００８４】ステップ４０７の処理で、セキュリティコードに対応するコンピュータ操作環境を変更する処理を選択した場合には、ステップ４１７の処理に進み、コンピュータ操作環境を変更したいセキュリティコードを指定し、設定を変更したコンピュータ操作環境を登録リスト２１０に登録しなおす。

【００８５】ステップ４０３の処理で、受信したセキュリティコードと登録リスト２１０に登録されているセキュリティコードとを比較した結果、受信したセキュリティコードが登録リスト２１０に登録されている有効なセキュリティコードではない場合には、登録リスト２１０の変更は許可されない。

【００８６】以上の様に、本実施形態のコンピュータ不正使用防止装置では、コンピュータ１１０に複数のセキュリティコードを登録する機能と登録したセキュリティコードの内容を変更する機能とを備えているので、セキュリティキー１０１が不正に使用された場合に不正に使用されたセキュリティキー１０１を無効化することが可能である。

【００８７】また、本実施形態のコンピュータ不正使用

防止装置では、コンピュータ１１０のセキュリティキー１０１毎に有効範囲を設定する機能と前記の設定した有効範囲を変更する機能とを備えているので、管理者と利用者でセキュリティのレベルを変更することが可能である。

【００８８】図５は、本実施形態のコンピュータ不正使用防止装置のシステム起動ロック処理の処理手順を示すフローチャートである。

【００８９】図５に示す様に、本実施形態のコンピュータ不正使用防止装置のシステム起動ロック処理では、ステップ５０１の処理で、セキュリティキー１０１の信号出力装置１０４から送信したセキュリティコード信号１０６を、補助電源で動作中のコンピュータ１１０の信号入力装置１１２で受信し、ステップ５０２の処理で、受信したセキュリティコードと登録リスト２１０に登録されているセキュリティコードとを比較する。

【００９０】ステップ５０２の処理で、受信したセキュリティコードと登録リスト２１０に登録されているセキュリティコードとを比較した結果、受信したセキュリティコードが登録リスト２１０に登録されている有効なセキュリティコードである場合には、ステップ５０３の処理に進み、主電源を投入した後、ステップ５０４の処理に進み、コンピュータ１１０のシステム起動を行う。

【００９１】ステップ５０２の処理で、受信したセキュリティコードと登録リスト２１０に登録されているセキュリティコードとを比較した結果、受信したセキュリティコードが登録リスト２１０に登録されている有効なセキュリティコードではない場合には、主電源の投入及びシステム起動は行わない。

【００９２】前記の様に、本実施形態のコンピュータ不正使用防止装置によれば、セキュリティ管理処理部１１６のシステム起動ロック処理機能２０３により、有効なセキュリティキー１０１がない場合には、コンピュータ１１０のパワーオン及びシステム起動が行えないので、コンピュータ１１０の盗難等による不正使用を防止することが可能である。

【００９３】また、本実施形態のコンピュータ不正使用防止装置では、セキュリティ管理処理部１１６の機能のシステム起動ロック処理機能２０３により、有効なセキュリティコードを受信するとコンピュータ１１０のパワーオン及びシステム起動が行なわれ、有効なセキュリティコードに対応して予め設定したコンピュータ操作環境に切り替えるので、コンピュータ１１０の操作環境をセキュリティコードに対応した利用者ごとの使いやすい操作環境に切り替えることが可能である。

【００９４】図６は、本実施形態のコンピュータ不正使用防止装置の中断再開ロック処理の処理手順を示すフローチャートである。

【００９５】図６に示す様に、本実施形態のコンピュータ不正使用防止装置の中断再開ロック処理では、ステップ６０１の処理で、一定時間中に入出力装置１１４のキーボードまたはマウス等への入力が行われているかを調べ、入出力装置１１４への入力が行われていない場合には、ステップ６０２の処理に進み、入出力装置１１４のディスプレイの画面を消去した後、ステップ６０３の処理で、入出力装置１１４のキーボードやマウス等からの入力を停止する。

【００９６】ステップ６０４の処理で、セキュリティキー１０１の信号出力装置１０４から送信されたセキュリティコード信号１０６を、コンピュータ１１０の信号入力装置１１２で受信し、ステップ６０５の処理で、受信したセキュリティコードと登録リスト２１０に登録されているセキュリティコードとを比較する。

【００９７】ステップ６０５の処理で、受信したセキュリティコードと登録リスト２１０に登録されているセキュリティコードとを比較した結果、受信したセキュリティコードが登録リスト２１０に登録されている有効なセキュリティコードである場合には、ステップ６０６の処理に進み、入出力装置１１４のディスプレイの画面表示を再開した後、ステップ６０７の処理に進み、入出力装置１１４のキーボードやマウス等からの入力を受け付ける。

【００９８】ステップ６０５の処理で、受信したセキュリティコードと登録リスト２１０に登録されているセキュリティコードとを比較した結果、受信したセキュリティコードが登録リスト２１０に登録されている有効なセキュリティコードではない場合には、ステップ６０４の処理に戻る。

【００９９】前記の様に、本実施形態のコンピュータ不正使用防止装置によれば、セキュリティ管理処理部１１６の中断再開ロック処理機能２０４により、有効なセキュリティキー１０１がない場合には、中断されたコンピュータ１１０の入出力装置１１４からの入力動作の再開が行えないので、コンピュータ１１０の利用者が不在時または離席時に不正使用されることを防止することが可能である。

【０１００】図７は、本実施形態のコンピュータ不正使用防止装置のアプリケーション起動ロック処理の処理手順を示すフローチャートである。

【０１０１】図７に示す様に、本実施形態のコンピュータ不正使用防止装置のアプリケーション起動ロック処理では、ステップ７０１の処理で、コンピュータ１１０内あるいはネットワークで接続された他のコンピュータ内のアプリケーションソフトウェアを起動する起動要求が行われると、ステップ７０２の処理で、セキュリティキー１０１の信号出力装置１０４から送信されたセキュリティコード信号１０６をコンピュータ１１０の信号入力装置１１２で受信し、ステップ７０３の処理で、受信したセキュリティコードと登録リスト２１０に登録されているセキュリティコードとを比較する。

【０１０２】ステップ７０３の処理で、受信したセキュリティコードと登録リスト２１０に登録されているセキュリティコードとを比較した結果、受信したセキュリティコードが登録リスト２１０に登録されている有効なセキュリティコードである場合には、ステップ７０４の処理に進み、ステップ７０１の処理で起動要求が行われているアプリケーションソフトウェアの起動を行う。

【０１０３】ステップ７０３の処理で、受信したセキュリティコードと登録リスト２１０に登録されているセキュリティコードとを比較した結果、受信したセキュリティコードが登録リスト２１０に登録されている有効なセキュリティコードではない場合には、ステップ７０１の処理で起動要求が行われているアプリケーションソフトウェアの起動を行わない。

【０１０４】図８は、本実施形態のコンピュータ不正使用防止装置のファイルロック処理の処理手順を示すフローチャートである。

【０１０５】図８に示す様に、本実施形態のコンピュータ不正使用防止装置のファイルロック処理では、ステップ８０１の処理で、コンピュータ１１０の外部記憶装置１１５内あるいはネットワークで接続された他のコンピュータ内に格納されているファイル１１７を操作するファイル操作要求が行われると、ステップ８０２の処理で、セキュリティキー１０１の信号出力装置１０４から送信されたセキュリティコード信号１０６をコンピュータ１１０の信号入力装置１１２で受信し、ステップ８０３の処理で、受信したセキュリティコードと登録リスト２１０に登録されているセキュリティコードとを比較する。

【０１０６】ステップ８０３の処理で、受信したセキュリティコードと登録リスト２１０に登録されているセキュリティコードとを比較した結果、受信したセキュリティコードが登録リスト２１０に登録されている有効なセキュリティコードである場合には、ステップ８０４の処理に進み、ステップ８０１の処理でファイル操作要求が行われているファイル１１７への操作を実行する。

【０１０７】ステップ８０３の処理で、受信したセキュリティコードと登録リスト２１０に登録されているセキュリティコードとを比較した結果、受信したセキュリティコードが登録リスト２１０に登録されている有効なセキュリティコードではない場合には、ステップ８０１の処理でファイル操作要求が行われているファイル１１７への操作を実行しない。

【０１０８】前記の様に、本実施形態のコンピュータ不正使用防止装置では、セキュリティ管理処理部１１６の機能のファイルロック処理機能２０６により、有効なセキュリティキー１０１がない場合には、ファイル１１７の操作が行えなくなり、有効なセキュリティコードを受信した後にファイル操作要求を実行するので、コンピュータ１１０内のファイル１１７の不正使用を防止することが可能である。

【０１０９】図９は、本実施形態のコンピュータ不正使用防止装置の暗号化処理の処理手順を示すフローチャートである。

【０１１０】図９に示す様に、本実施形態のコンピュータ不正使用防止装置の暗号化処理では、コンピュータ１１０内あるいはネットワークで接続された他のコンピュータ内のファイル１１７や通信電文などを暗号化するときに、ステップ９０１の処理で、コンピュータ１１０のセキュリティ管理処理部１１６の暗号化処理機能２０７を呼び出し、暗号化処理機能２０７を起動する。

【０１１１】ステップ９０２の処理で、セキュリティキー１０１の信号出力装置１０４から送信されたセキュリティコード信号１０６をコンピュータ１１０の信号入力装置１１２で受信し、ステップ９０３の処理で、受信したセキュリティコードに基づいて暗号化処理を実行する。

【０１１２】図１０は、本実施形態のコンピュータ不正使用防止装置の復号化処理の処理手順を示すフローチャートである。

【０１１３】図１０に示す様に、本実施形態のコンピュータ不正使用防止装置の復号化処理では、コンピュータ１１０内あるいはネットワークで接続された他のコンピュータ内の暗号化されたファイル１１７や通信電文などを復号化するときに、ステップ１００１の処理で、コンピュータ１１０のセキュリティ管理処理部１１６の復号化処理機能２０８を呼び出し、復号化処理機能２０８を起動する。

【０１１４】ステップ１００２の処理で、セキュリティキー１０１の信号出力装置１０４から送信されたセキュリティコード信号１０６をコンピュータ１１０の信号入力装置１１２で受信し、ステップ１００３の処理で、受信したセキュリティコードに基づいて復号化処理を実行する。

【０１１５】前記の様に、本実施形態のコンピュータ不正使用防止装置では、セキュリティ管理処理部１１６の暗号化処理機能２０７と復号化処理機能２０８とにより、コンピュータ１１０内の情報の暗号化及び復号化を行うので、コンピュータ１１０内およびネットワーク等で接続された他のコンピュータ内のデータやアプリケーションソフトウェア等の情報の不正使用を防止することが可能である。

【０１１６】図１１は、本実施形態のコンピュータ不正使用防止装置の使用状況の履歴取得処理の処理手順を示すフローチャートである。

【０１１７】図１１に示す様に、本実施形態のコンピュータ不正使用防止装置の使用状況の履歴取得処理では、ステップ１１０１の処理で、入出力装置１１４からの入力が行われたときに、ステップ１１０２の処理で、登録リスト２１０に登録されている有効なセキュリティコー

ドを受信済みであるかどうかを調べる。

【００１８】ステップ１１０２の処理で、登録リスト２１０に登録されている有効なセキュリティコードを受信済みであるかどうかを調べた結果、有効なセキュリティコードが受信されていない場合には、ステップ１１０１の処理で入出力装置１１４に入力された内容を、コンピュータ１１０の使用状況の履歴として、コンピュータ１１０の外部記憶装置１１５内あるいはネットワークで接続された他のコンピュータ内の履歴ファイルに記憶する。

【００１９】前記の様に、本実施形態のコンピュータ不正使用防止装置では、セキュリティ管理処理部１１６の機能の使用状況の履歴取得処理機能２０９により、有効なセキュリティキー１０１がない場合には、コンピュータ１１０の使用状況の履歴を記憶するので、コンピュータ１１０の不正使用を行おうとする操作が全て記録されることを示すことにより、コンピュータ１１０の不正使用を直接防止するのでなく、コンピュータ１１０の不正使用を行おうとする試みを抑止することが可能である。

【００２０】また、本実施形態のコンピュータ不正使用防止装置では、セキュリティキー１０１のセキュリティコードをネットワーク通信におけるアクセス元を認証する為のワンタイムパスワードとして応用することにより、ネットワークを使用した不正な通信を防止することが可能である。

【００２１】すなわち、ネットワークを使用してアクセスするアクセス元は、このネットワークから初めにアクセス元に送られた固定的でないコードとアクセス元のセキュリティコードと間で一定の計算を行った結果、例えば、イクスクルーシブオアを行った計算結果をそのアクセスに使用するパスワードとし、ネットワーク側は、このパスワードと初めに送ったコード間でさらにイクスクルーシブオアの計算を行えば、セキュリティコードを得ることができ、アクセス元を認証することが可能である。このとき、ネットワークから初めに送られるコードは毎回変わる為、アクセスに使用するパスワードも毎回変わり、そのパスワードが盗聴されても不正に使用することができない。

【００２２】以上説明した様に、本実施形態のコンピュータ不正使用防止装置によれば、発生したユニークなセキュリティコードを出力してコンピュータのセキュリティ管理を行うので、コンピュータの不正使用を防止するセキュリティ管理の操作性を向上することが可能である。

【００２３】（実施形態２）以下に、本発明のコンピュータ不正使用防止装置において、ＩＣカードのセキュリティキーを使用する実施形態２のコンピュータ不正使用防止装置について説明する。

【００２４】図１２は、本実施形態のコンピュータ不正使用防止装置の概略構成を示す図である。図１２において、１２００はセキュリティキー、１２０１はＩＣカード側信号入力装置、１２１０はＩＣカードリーダライタ、１２１１はＩＣカードリーダライタ側信号出力装置である。

【００２５】図１２に示す様に、本実施形態のコンピュータ不正使用防止装置は、セキュリティキー１２００と、ＩＣカード側信号入力装置１２０１と、ＩＣカードリーダライタ１２１０と、ＩＣカードリーダライタ側信号出力装置１２１１とを有している。

【００２６】また、図１２に示す様に、本実施形態のコンピュータ不正使用防止装置では、ＩＣカードであるセキュリティキー１２００を使用して、コンピュータ１１０のセキュリティ管理を行う。

【００２７】本実施形態のコンピュータ不正使用防止装置のセキュリティキー１２００は、コンピュータ１１０から出力されるセキュリティコード等の情報を入力するＩＣカード側信号入力装置１２０１に備えており、また、コンピュータ１１０のＩＣカードリーダライタ１２１０は、セキュリティキー１２００にセキュリティコード等の情報を出力するＩＣカードリーダライタ側信号出力装置１２１１を備えている。

【００２８】図１３は、本実施形態のコンピュータ不正使用防止装置のセキュリティ管理処理部１１６の概略構成を示す図である。図１３において、１３０１はセキュリティコード変更処理機能である。

【００２９】図１３に示す様に、本実施形態のコンピュータ不正使用防止装置のセキュリティ管理処理部１１６は、セキュリティコード変更処理機能１３０１を有している。

【００３０】本実施形態のコンピュータ不正使用防止装置のセキュリティ管理処理部１１６は、実施形態１に示した複数の処理機能に加え、登録リスト２１０に登録された特定のセキュリティコードと、セキュリティキー１２００に記憶されているセキュリティコードとを同時に変更するセキュリティコード変更処理機能１３０１を備えている。

【００３１】本実施形態のコンピュータ不正使用防止装置では、ＩＣカードで構成されたセキュリティキー１２００のセキュリティコード発生装置１０３から発生されたユニークなセキュリティコードを特定のセキュリティコード信号に変換し、前記変換したセキュリティコード信号をコンピュータ１１０のＩＣカードリーダライタ１２１０の信号入力装置１１２に出力する。

【００３２】コンピュータ１１０の信号入力装置１１２は、セキュリティキー１２００の信号出力装置１０４から送られてきたセキュリティコード信号を入力してセキュリティコードに変換し、コンピュータ１１０のセキュリティ管理処理部１１６は、登録リスト２１０を参照して、前記変換したセキュリティコードが有効なセキュリティコードであるかどうかの照合判定を行う。

【００１３】前記変換したセキュリティコードが有効なセキュリティコードである場合には、前記セキュリティコードに対応する特定の機能の実行を許可し、また、前記変換したセキュリティコードが有効なセキュリティコードでない場合には、前記コンピュータ１１０の使用を禁止する。

【００１４】また、セキュリティ管理処理部１１６は、前記変換したセキュリティコードが有効なセキュリティコードである場合に、セキュリティコードを変更するセキュリティコード変更処理機能１３０１が選択されると、登録リスト２１０中の対応するセキュリティコードを変更すると共に、コンピュータ１１０のＩＣカードリーダライタ側信号出力装置１２１１により、前記変更したセキュリティコードをセキュリティコード信号に変換してセキュリティキー１２００に出力する。

【００１５】セキュリティキー１２００のＩＣカード側信号入力装置１２０１は、コンピュータ１１０のＩＣカードリーダライタ側信号出力装置１２１１から送られてきたセキュリティコード信号を入力してセキュリティコードに変換し、前記変換したセキュリティコードを使用してセキュリティキー１２００のセキュリティコード発生装置１０３が発生するセキュリティコードを変更する。

【００１６】また、前記の様にＩＣカードを使用してセキュリティキー１２００を高機能化し、コンピュータ１１０のＩＣカードリーダライタ側信号出力装置１２１１及びセキュリティキー１２００のＩＣカード側信号入力装置１２０１を使用することにより、コンピュータ１１０の使用履歴情報や障害情報をセキュリティキー１２００に蓄積したり、また、セキュリティ管理だけでなく、勤怠情報を蓄積して勤怠管理に使用したり、製品情報を蓄積して在庫管理に使用し、また、現金情報を蓄積して電子マネーと兼用することが可能である。

【００１７】以上説明した様に、本実施形態のコンピュータ不正使用防止装置によれば、コンピュータの信号出力装置により変更したセキュリティコードをセキュリティキーに出力し、セキュリティキーのセキュリティコードを変更するので、セキュリティの強度を向上せさることが可能である。

【００１８】（実施形態３）以下に、本発明のコンピュータ不正使用防止装置において、ネットワークに接続された他のコンピュータのセキュリティ管理を行う実施形態３のコンピュータ不正使用防止装置について説明する。

【００１９】図１４は、本実施形態のコンピュータ不正使用防止装置の概略構成を示す図である。図１４において、１４０１はセキュリティコード送信部、１４１０はコンピュータ、１４１１はセキュリティコード受信部である。

【００２０】図１４に示す様に、本実施形態のコンピュータ不正使用防止装置は、セキュリティコード送信部１４０１と、コンピュータ１４１０と、セキュリティコード受信部１４１１とを有している。

【００２１】また、図１４に示す様に、本実施形態のコンピュータ不正使用防止装置では、ネットワークを介して接続されたコンピュータ１４１０のセキュリティ管理を、コンピュータ１１０から行う構成を表している。

【００２２】本実施形態のコンピュータ不正使用防止装置のコンピュータ１１０は、ネットワークを介してコンピュータ１４１０にセキュリティコードを送信するセキュリティコード送信部１４０１を備え、また、コンピュータ１４１０は、ネットワークを介してコンピュータ１１０から送信されたセキュリティコードを受信するセキュリティコード受信部１４１１を備えている。

【００２３】図１５は、本実施形態のコンピュータ不正使用防止装置のセキュリティ管理処理部１１６の概略構成を示す図である。図１５において、１５０１は他システム管理処理機能である。

【００２４】図１５に示す様に、本実施形態のコンピュータ不正使用防止装置のセキュリティ管理処理部１１６は、他システム管理処理機能１５０１を有している。

【００２５】本実施形態のコンピュータ不正使用防止装置のセキュリティ管理処理部１１６は、実施形態１に示した複数の処理機能に加え、ネットワークを介して接続されたコンピュータ１４１０のセキュリティ管理を行う他システム管理処理機能１５０１を備えている。

【００２６】本実施形態のコンピュータ不正使用防止装置では、セキュリティキー１０１から受信したセキュリティコードが有効なセキュリティコードである場合に、コンピュータ１４１０のセキュリティ管理を実行する他システム管理処理機能１５０１が選択されると、セキュリティコード送信部１４０１により、セキュリティキー１０１から受信済みの有効なセキュリティコードをネットワークに接続されたコンピュータ１４１０に送信する。

【００２７】ネットワークに接続されたコンピュータ１４１０は、セキュリティコード受信部１４１１によりセキュリティコードを受信した後、コンピュータ１４１０のセキュリティ管理処理部１１６を起動する。

【００２８】セキュリティコード送信部１４０１によりセキュリティコードを送信したコンピュータ１１０は、前記起動されたコンピュータ１４１０のセキュリティ管理処理部１１６に、セキュリティ管理に関する指示を送り、コンピュータ１４１０のセキュリティ管理機能を実行する。

【００２９】以上説明した様に、本実施形態のコンピュータ不正使用防止装置によれば、ネットワークに接続された他のコンピュータのセキュリティ管理処理を実行するので、セキュリティキーからのセキュリティコード信号を入力するインタフェースを備えていないコンピュー

タに対してもセキュリティ管理を行うことが可能である。

【００１５０】以上、本発明を前記実施形態に基づき具体的に説明したが、本発明は、前記実施形態に限定されるものではなく、その要旨を逸脱しない範囲において種々変更可能であることは勿論である。

【００１５１】

【発明の効果】本願において開示される発明のうち代表的なものによって得られる効果を簡単に説明すれば、下記のとおりである。

【００１５２】（１）発生したユニークなセキュリティコードを出力してコンピュータのセキュリティ管理を行うので、コンピュータの不正使用を防止するセキュリティ管理の操作性を向上することが可能である。

【００１５３】（２）コンピュータの信号出力装置により変更したセキュリティコードをセキュリティキーに出力し、セキュリティキーのセキュリティコードを変更するので、セキュリティの強度を向上せさることが可能である。

【００１５４】（３）ネットワークに接続された他のコンピュータのセキュリティ管理処理を実行するので、セキュリティキーからのセキュリティコード信号を入力するインタフェースを備えていないコンピュータに対してもセキュリティ管理を行うことが可能である。

【図面の簡単な説明】

【図１】実施形態１のコンピュータ不正使用防止装置の概略構成を示す図である。

【図２】実施形態１のコンピュータ不正使用防止装置のセキュリティ管理処理部１１６の概略構成を示す図である。

【図３】実施形態１のコンピュータ不正使用防止装置のセキュリティコードの登録処理の処理手順を示すフローチャートである。

【図４】実施形態１のコンピュータ不正使用防止装置のセキュリティコードの変更処理の処理手順を示すフローチャートである。

【図５】実施形態１のコンピュータ不正使用防止装置のシステム起動ロック処理の処理手順を示すフローチャートである。

【図６】実施形態１のコンピュータ不正使用防止装置の中断再開ロック処理の処理手順を示すフローチャートである。

【図７】実施形態１のコンピュータ不正使用防止装置のアプリケーション起動ロック処理の処理手順を示すフローチャートである。

【図８】実施形態１のコンピュータ不正使用防止装置のファイルロック処理の処理手順を示すフローチャートである。

【図９】実施形態１のコンピュータ不正使用防止装置の暗号化処理の処理手順を示すフローチャートである。

【図１０】実施形態１のコンピュータ不正使用防止装置の復号化処理の処理手順を示すフローチャートである。

【図１１】実施形態１のコンピュータ不正使用防止装置の使用状況の履歴取得処理の処理手順を示すフローチャートである。

【図１２】実施形態２のコンピュータ不正使用防止装置の概略構成を示す図である。

【図１３】実施形態２のコンピュータ不正使用防止装置のセキュリティ管理処理部１１６の概略構成を示す図である。

【図１４】実施形態３のコンピュータ不正使用防止装置の概略構成を示す図である。

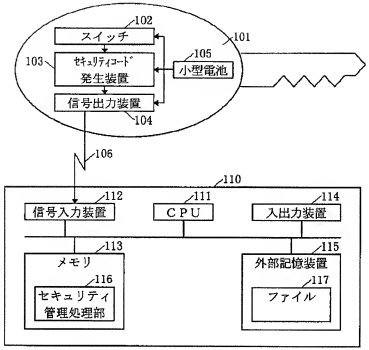
【図１５】実施形態３のコンピュータ不正使用防止装置のセキュリティ管理処理部１１６の概略構成を示す図である。

【符号の説明】

１０１…セキュリティキー、１０２…スイッチ、１０３…セキュリティコード発生装置、１０４…信号出力装置、１０５…小型電池、１０６…セキュリティコード信号、１１０…コンピュータ、１１１…ＣＰＵ、１１２…信号入力装置、１１３…メモリ、１１４…入出力装置、１１５…外部記憶装置、１１６…セキュリティ管理処理部、１１７…ファイル、２０１…登録処理機能、２０２…変更処理機能、２０３…システム起動ロック処理機能、２０４…中断再開ロック処理機能、２０５…アプリケーション起動ロック処理機能、２０６…ファイルロック処理機能、２０７…暗号化処理機能、２０８…復号化処理機能、２０９…使用状況の履歴取得処理機能、２１０…登録リスト、１２００…セキュリティキー、１２０１…ＩＣカード側信号入力装置、１２１０…ＩＣカードリーダライタ、１２１１…ＩＣカードリーダライタ側信号出力装置、１３０１…セキュリティコード変更処理機能、１４０１…セキュリティコード送信部、１４１０…コンピュータ、１４１１…セキュリティコード受信部、１５０１…他システム管理処理機能。

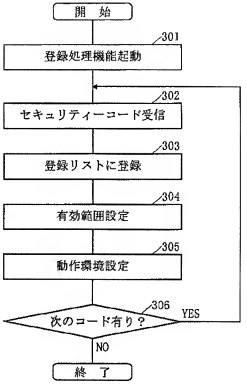
【図１】

図１



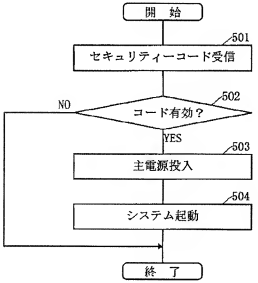
【図３】

図３



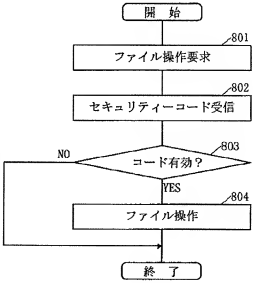
【図５】

図５



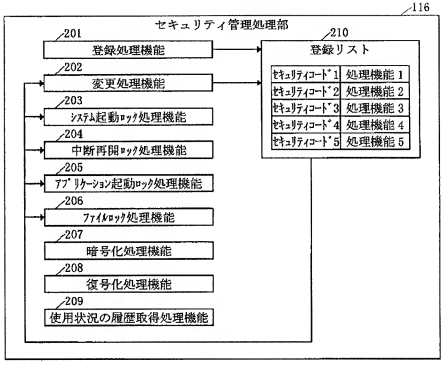
【図８】

図８



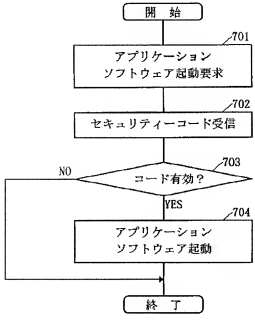
【図2】

図2



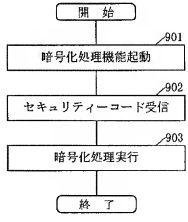
【図7】

図7



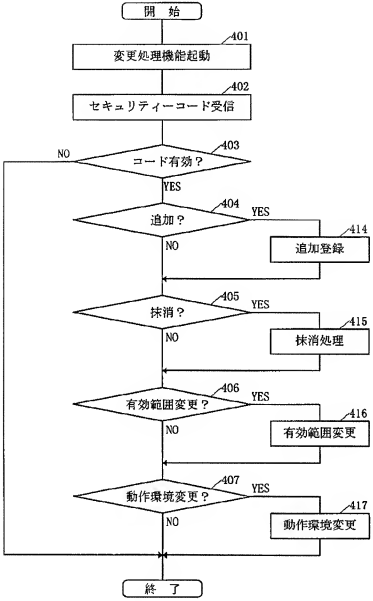
【図9】

図9



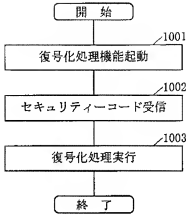
【図４】

図４


開　始
401
変更処理機能起動
402
セキュリティーコード受信
403
コード有効？
NO
YES
404
追加？
YES
414
追加登録
NO
405
抹消？
YES
415
抹消処理
NO
406
有効範囲変更？
YES
416
有効範囲変更
NO
407
動作環境変更？
YES
417
動作環境変更
NO
終　了

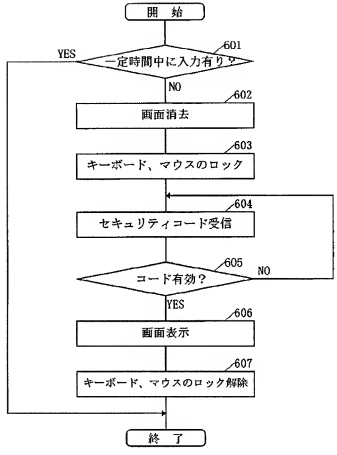
【図１０】

図１０


開　始
1001
復号化処理機能起動
1002
セキュリティーコード受信
1003
復号化処理実行
終　了

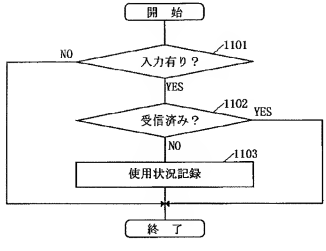
【図6】

図6


開　始
601
一定時間中に入力有り？
YES
NO
602
画面消去
603
キーボード、マウスのロック
604
セキュリティコード受信
605
コード有効？
NO
YES
606
画面表示
607
キーボード、マウスのロック解除
終　了

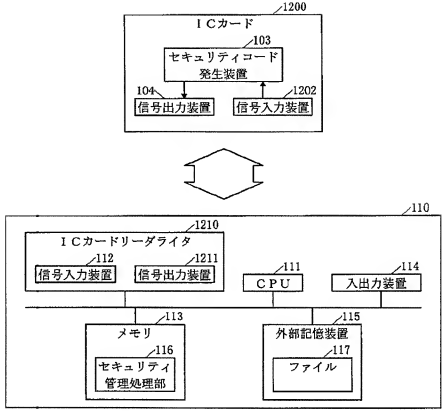
【図11】

図11


開　始
1101
入力有り？
NO
YES
1102
受信済み？
YES
NO
1103
使用状況記録
終　了

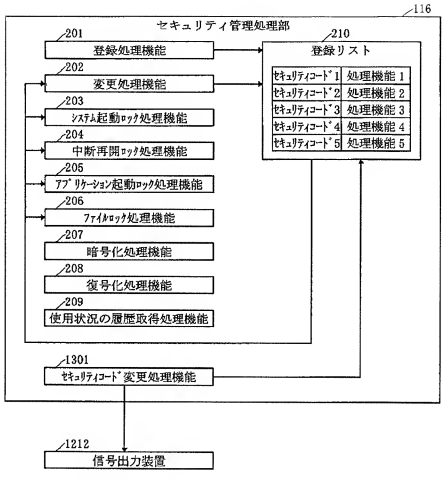
【図１２】

図１２


1200
ＩＣカード
103
セキュリティコード
発生装置
104
信号出力装置
1202
信号入力装置
110
1210
ＩＣカードリーダライタ
112
信号入力装置
1211
信号出力装置
111
ＣＰＵ
114
入出力装置
113
メモリ
116
セキュリティ
管理処理部
115
外部記憶装置
117
ファイル

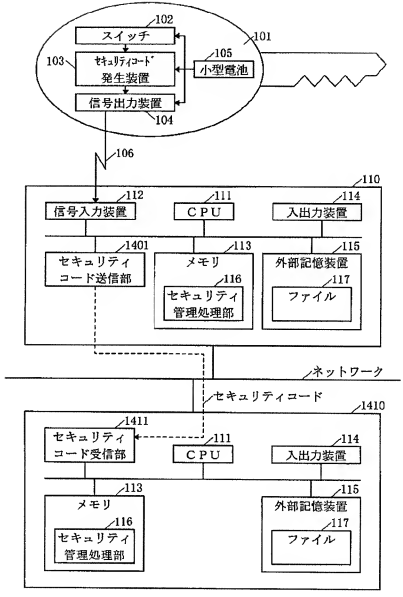
【図13】

図13


116
セキュリティ管理処理部
201
登録処理機能
202
変更処理機能
203
ｼｽﾃﾑ起動ﾛｯｸ処理機能
204
中断再開ﾛｯｸ処理機能
205
ｱﾌﾟﾘｹｰｼｮﾝ起動ﾛｯｸ処理機能
206
ﾌｧｲﾙﾛｯｸ処理機能
207
暗号化処理機能
208
復号化処理機能
209
使用状況の履歴取得処理機能
210
登録リスト
ｾｷｭﾘﾃｨｺｰﾄﾞ1 処理機能1
ｾｷｭﾘﾃｨｺｰﾄﾞ2 処理機能2
ｾｷｭﾘﾃｨｺｰﾄﾞ3 処理機能3
ｾｷｭﾘﾃｨｺｰﾄﾞ4 処理機能4
ｾｷｭﾘﾃｨｺｰﾄﾞ5 処理機能5
1301
ｾｷｭﾘﾃｨｺｰﾄﾞ変更処理機能
1212
信号出力装置

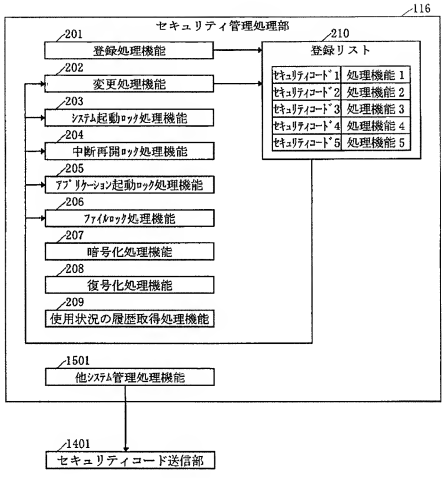
【図１４】

図１４


102
スイッチ
101
105
103
ｾｷｭﾘﾃｨｺｰﾄﾞ
発生装置
小型電池
信号出力装置
104
106
110
112
信号入力装置
111
ＣＰＵ
114
入出力装置
1401
セキュリティ
コード送信部
113
メモリ
115
外部記憶装置
116
セキュリティ
管理処理部
117
ファイル
ネットワーク
セキュリティコード
1410
1411
セキュリティ
コード受信部
111
ＣＰＵ
114
入出力装置
113
メモリ
115
外部記憶装置
116
セキュリティ
管理処理部
117
ファイル

【図１５】

図１５


116
セキュリティ管理処理部
201
登録処理機能
210
登録リスト
セキュリティコード1
処理機能1
セキュリティコード2
処理機能2
セキュリティコード3
処理機能3
セキュリティコード4
処理機能4
セキュリティコード5
処理機能5
202
変更処理機能
203
システム起動ロック処理機能
204
中断再開ロック処理機能
205
アプリケーション起動ロック処理機能
206
ファイルロック処理機能
207
暗号化処理機能
208
復号化処理機能
209
使用状況の履歴取得処理機能
1501
他システム管理処理機能
1401
セキュリティコード送信部